A Psychological Approach to Information Security

Some Ideas for Establishing Information Security Psychology

Katsuya Uchida(✉)

Institute of Information Security, Yokohama, Japan
uchidak@gol.com

Abstract. Information Systems are composed in four main portions, people, information, appliance and facilities. These four portions are called information assets. Information security protects information assets and keeps safe them from the view point of Confidentiality, Integrity and Availability (CIA).

Recently, cyber-attacks to people in specific organizations are called advanced persistent threat (APT) or targeted attacks. APT attacks are attacks using psychological and behavioral science weakness of people, are not technical attacks.

Kevin Mitnick, the most competent and the most famous attacker for people says "Security is not a technology problem. It is a human and management problems" in his book.

By using the knowledge of psychology, behavioral science and criminology, the attackers attack people, and achieve the purposes. Targets of the attacks are not only the direct objects that are theft or destruction of information, but also the indirect objects that obtain the information necessary to achieve the goal.

Sun Tzu, a Chinese military general, strategist and philosopher said "If you know your enemies and know yourself, you can win a hundred battles without a single loss".

Attackers and victims are classified into people, appliance (hardware and software) and hybrid (people and appliance).

The methods of attackers for each attack and cases of attacks are classified in this paper.

Some organizations are beginning to use the elements of games and competitions to motivate employees, and customers. This is known as gamification which is the application of game elements and digital game design techniques to non-game problems, such as business and social impact challenges.

Gamification is very useful for awareness training of information security, I believe.

M. Kurosu (Ed.): Human-Computer Interaction, Part I, HCII 2015, LNCS 9169, pp. 96–104, 2015.
DOI: 10.1007/978-3-319-20901-2_9

This paper attempts to classify and systematize attackers, victims and the methods of attacks, as by psychology, behavioral science, criminal psychology, and cognitive psychology I have proposed some ideas for education, training and awareness for information security using the findings of psychology and behavioral science.

Keywords: Information security psychology · Social engineering · Deception

1 Introduction

Information security psychology is to research the information security from the human aspects or psychology.

Information security is to protect information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity and availability.

The attacker is to attack victims by using the findings of psychology, behavioral science and criminology. The objective of attack is to be a theft or destruction of information assets, and to obtain information to achieve the final goal.

Defenders acquire the knowledge that the attackers use, and must think about the defense systems. By performing the education and training, etc. for the user of the information assets, it is necessary to consider measures to protect the information assets from the attacker. By using the knowledge of psychology, behavioral science, and criminology, effective education and training are performed.

In education and training, we have two areas:

- One is that the course contents include knowledge of psychology, behavioral science and criminology.
- The other one is that the design of education and training include psychological concepts, especially regarding motivation, behavior, and personality.

2 Information Assets

2.1 Definition of Information Assets

The following are definition of the information assets which are classified with the four groups [1].

- **People** are those who are vital to the expected operation and performance of the service. People may be internal or external to the organization.
- **Information** is any information or data, on any media including paper or electronic form.
- **Technology** describes any technology component or asset that supports or automates a service and facilitates its ability to accomplish its mission. Some technology are specific to a service (such as an application system) and others are shared by the organization (such as the enterprise-wide network infrastructure).

- **Facilities** are the places where services are executed and can be owned and controlled by the organization or by external business partners. In general, any of the information assets are targeted attackers and many of the cyber-attacks use the findings of psychology and behavioral science as well as the technical knowledge.

2.2 Attacks of Deception Against Information Assets

In general, any of the information assets are targeted attackers and many of the cyber-attacks use the findings of psychology and behavioral science as well as the technical knowledge.

The following are the psychological and behavioral scientific attacks for each group.

- **People:** Attacker makes a call by pretending to be someone else and gets the necessary information.
- **Information:** One example is a targeted attack which has been aimed at a specific user, company or organization using e-mail of attached file or embedded url.
- **Technology:** A SYN flood attack is intended to deceive the three-way handshake of TCP, that is, this attack works by not responding to the server with the expected ACK code.
- **Facilities:** Attacker enters premises by pretending to people of a delivery company or an electrical work company, and often looks for information discarded by a company employees.

3 Basic Model of the Deception

From time immemorial, human beings have been deceived others. Recently, some people begin to deceive new field, computer systems. Directly, some people deceive other people related to the computer systems instead of deceiving the computer systems.

In the information security, we call this social engineering.

1. **Definition of Social Engineering**

Some definitions for social engineering are as follow;

- Social engineering refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional “con” in that it is often one of many steps in a more complex fraud scheme [2].
- Social engineering is the act of manipulating a person to take an action that may or may not be in the “target” best interest. This may include obtaining information, gaining access, or getting the target to take certain action [3].

I would like to take a further more wide definition, that is, social engineering or the art of the deception is the act of manipulating person and/or things to take an action that may or may not be in the target best interest.

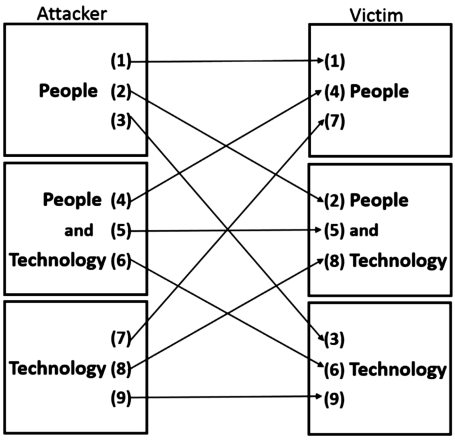

Fig. 1. Basic model of deception

2. **Basic model of deception**

Figure 1 shows the relationship between attacker and victim. Attacker and victim are classified three group, People, Technology, and People and technology.

Each group of attackers deceives each group of victims by social engineering techniques

(1) "People" attacks "People"
This is mainstream part in social engineering. There are phone call with victim, URL embedded e-mail, and targeted email attack induced by message exchange.
(2) "People" attacks "People and Technology"
Shoulder hacking and site intrusion are famous in this attack.
(3) "People'" attacks "Technology"
Biometrics system authenticates the fake biometric, such as fingerprint.
(4) "People and technology" attacks "People"
Vishing (Voice phishing) uses telephone system for automatic call and attacker's voice.
(5) "People and technology" attacks "People"
Nothing special.
(6) "People and technology" attacks "People and technology"
The e-mail attached with malware is this area.
(7) "Technology" attacks "People"
Caller ID spoofing is the practice of causing the telephone network to indicate to the receiver of a call that the originator of the call is a station other than the true originating station.
(8) "Technology" attacks "People and technology"

Malware is malicious code that includes viruses, worms, and Trojan horses.

(9) "Technology" attacks "Technology"

- SYN Flooding deceives TCP connections that are designed to perform the 3-way handshake with the server and the client.
- Mac spoofing is a technique for changing a factory-assigned Media Access Control (MAC) address of a network interface on a networked device.

4 Some Cases for Social Engineering

Some cases for the art of deception are as follow.

(1) Oct. 1981, "Fake phone call" at Japanese Local bank1The attacker was a phone call "I am a member of COMCEN (the local bank jargon, "computer center") so please make fund transfer 35 million yen to the account of S branch for computer test." The manager in Savings account department believed the phone call from the data center, and made fund transfer. After the fund transfer, a female accomplice withdrew 30 million yen from the account in S branch.

(2) Dec. 1987, Forged sender address (Mail spoofing) CHRISTMAS.exe worm
A user would receive an e-mail Christmas card that included executable code. If executed the program claimed to draw a Xmas tree on the display. It also sent a copy to everyone on the user's address lists.

(3) Nov. 2011, "DARPA Shredder challenge" for Dumpster diving [4]
Dumpster diving is the most exciting thing for attackers, they can find a lot of valuables, CD-ROM, USB memory, and user manual, etc., in dumpsters.
Straight cut of documents by a shredder was restored by Iranian students about 35 years ago. Cross cut documents by recent shredder was also restored at DARPA's Shredder challenge in Dec. 2011.

(4) Shoulder hacking
From some results of the simple experimental, shoulder hacking is very difficult without the recording of the video or photo.
Therefore, you can see ATM skimming instead of shoulder hacking. ATM skimming is when someone illegally copies your account details from the magnetic strip on your credit or debit card when you use an ATM. Card skimming can also happen when you use ATM.2.

(5) Pretexting
At the request of a private detective hired by the stalker, the executive of a research company who pretended to be the housewife husband, telephoned some city hall in Japan on the day before the murder occurred and got the information of the housewife.
In leakage of personal information from the city hall, the stalker killed a housewife, and also killed himself [5].

(6) Microexpressions

A microexpression is a brief, involuntary facial expression shown on the face of humans.
They express the six universal emotions: disgust, anger, fear, sadness, happiness, and surprise. They are very brief in duration, lasting only 1/25 to 1/15 of a second.
A social engineer understands the true feelings from microexpression of the victim.
Example of microexpression, I know only in the movie series, "Lie to me".

5 Psychological Findings Used in Social Engineering

It most important response to social engineering is to understand how social engineers to use what kind of psychological findings.

5.1 Six Weapons of Influence

Cialdini has been written compliance techniques into six categories based on psychological findings that direct human behavior [6].

(1) Reciprocation recognizes that people feel indebted to those who do something for them or give them a gift.
(2) Commitment and Consistency
   (a) Low-ball technique is a technique used in sales and other styles of persuasion to offer products or services at a bargain price in order to first attract a buyer, but then adds on additional expenses to make the purchase less of a bargain than originally thought.
   (b) Door-in-the-face technique is to make a costly large first request that the recipient will probably refuse, and then is to make less costly and more realistic request.
   (c) Foot-in-the-door technique is the tendency for people to comply with some large request after first agreeing to a small request.
(3) Social Proof: When people are uncertain about a course of action, they tend to look to those around them to guide their decisions and actions.
(4) Liking: People prefer to say 'yes' to people who are attractive, similar to themselves, or who give them compliments.
(5) Authority: People want to follow the lead of real experts.
(6) Scarcity: The more rare and uncommon a thing, the more people want it.

5.2 Elicitation

The following is the definition of elicitation by FBI [7]

Elicitation is a technique used to discreetly gather information.
Elicitation is to extract information from people without giving them the feeling they are being interrogated.

A trained elicitor understands certain human or cultural predispositions and uses techniques to exploit those.

An elicitor is an excellent communicator.

Mentioned before at 4.(5) pretexting, the executive of a research company was good elicitor.

5.3 Environmental Criminology

A criminal is a normal ordinary people who is a weak presence in the temptation of crime opportunity. Many people have weak characteristic that would not resist temptation and suffering.

6 Education and Training

6.1 Education, Training, and Awareness

(1) Against Pretexting

As personal information leakage countermeasures, we hold an awareness training as follow.

As actually an example that occurred, an awareness training introduces a telephone deception technique by the attacker, and the characteristics of the victims. From the introduced contents, at the awareness training, we discuss what the victims should be done in this situation with taking into account the characteristics of the attacker and the victims.

An example of characteristics of an attacker and a victim are as follow;

- Attacker
  - Posting as a housewife husband or a fellow employee
  - Using insider lingo and terminology to gain trust
  - Refuse to give call back number, and ask to call mobile phone number
  - Stress urgency
- Victims
  - believe kindness and politeness are good for his or her customers
  - tend to trust others
  - do not want to involve with the problem
  - become a feeling that perpetrators want going well.

(2) Training a targeted attack

A targeted attack is designed to test employees' level of user awareness or their detection and response capabilities.

First step: from the address of address spoofing, the email that attached a file is sent to employees. After the mail was sent, we count the number of employees who opened the attached file, and calculate the percentage of employees who opened it.

Second step: from the address of address spoofing, email of the embedded URL is

sent to employees. After the mail was sent, we count the number of employees who clicked the URL, and calculate the percentage of employees who clicked it.

6.2 Gamification

Werbach says that;

> *Gamification is the use of game elements and game design techniques in non-game contexts* [8].
> *Gamification is about learning, learning from game design but also learning from fields like psychology and management and marketing and economics.*
> *It's a way in to understand things about motivation.*

The best usage of gamification is security awareness training, so we are planning to the information security contents for business area.

7 Conclusion

As Sun Tzu said "If you know your enemies and know yourself, you can win a hundred battles without a single loss", basically, learning techniques of attackers is to be the best protection of social engineering.

In addition, Gamification become an effective tools to education, training, and awareness to improve the security level of the user.

Attack defense methods and education and training, properly I do well-known classification.

In addition, there is a need to crime characteristics of the crime, etc. both research from the side of criminal psychology deepen.

In this research, it is not able to sufficiently classification deceptive, if it is possible to consider dealing appropriate classification of new attacks method utilizing psychological or behavioral science, and lead to the establishment of information security Psychology

Acknowledgements. This research of the Information Security Psychology study group has been granted by the Japanese Psychological Association from 2011.

References

1. Caralli, R.A. et al.: CERT Resilience Management Model, version 1.0, pp. 4–5. Software Engineering Institute, Carnegie Mellon University, Pittsburgh (2010)
2. Wikipedia: Social engineering (security). http://en.wikipedia.org/wiki/Social_engineering_(security)
3. Hadnagy, R.: Social Engineering: The Art of Human Hacking. Wiley, New York (2010)
4. DARPA: DARPA's shredder challenge (2011). http://archive.darpa.mil/shredderchallenge/

5. Japan Times: Stalking victim info leak laid to tax man (2013). http://www.japantimes.co.jp/news/2013/11/08/national/crime-legal/stalking-victim-info-leak-laid-to-tax-man/#.VOC3g-_9n9Q
6. Cialdini, R.: Influence: Science and Practice. Prentice Hall, Needham (2008)
7. FBI: Elicitation techniques (2011). http://www.fbi.gov/about-us/investigate/counterintelligence/elicitation-techniques
8. Werbach, K., et al.: For the Win: How Game Thinking Can Revolutionize Your Business. Wharton Digital Press, Philadelphia (2012)
9. Thornton, D., et al.: Gamification of information systems and security training: issues and case studies. Inf. Secur. Educ. J. **1**(1), 16–24 (2014)